AFFIDAVIT IN SUPPORT OF AN APPLICATION FOR A SEARCH WARRANT

I, Daniel E. Zaehringer, a Special Agent (SA) with Homeland Security Investigations (HSI), being duly sworn, depose and state as follows:

INTRODUCTION

1. I have been employed as a Special Agent of the U.S. Department of Homeland Security, Homeland Security Investigations (HSI) since 2010, and am currently assigned to the HSI Bangor, Maine office. Since 2015, I have investigated crimes involving the use of computers and the Internet and have investigated crimes involving the sexual exploitation of children. I have participated in the execution of numerous search warrants, both residential and online accounts, and the seizure of computers, cell phones, electronic media, and other items evidencing violations of federal laws pertaining to the sexual exploitation of children. I have also participated in numerous arrests and interviews of subjects involved with child exploitation and/or child pornography and have reviewed numerous examples of child pornography (as defined in 18 U.S.C. § 2256) in all forms of media including computer media. As an HSI agent, I am authorized to conduct these investigations and to request and execute search warrants for evidence of violations of Title 18 of the United States Code.

2. This affidavit is submitted in support of an application for a search warrant for the locations specifically described in Attachment A of this Affidavit and any devices seized, including the entire property located at 52 Park Street, East Millinocket, Maine,

04430 (the "SUBJECT PREMISES") for contraband and evidence, fruits, and instrumentalities of violations of Title 18, United States Code, Sections 2252 and 2252A which are more specifically described in Attachment B of this Affidavit.

3. The facts set forth in this affidavit are based on my personal knowledge, information obtained during my participation in this investigation, information from others, including law enforcement officers, my review of documents and computer records related to this investigation, and information gained through my training and experience. Based on this training and experience, there is probable cause to believe that contraband and evidence, fruits, and instrumentalities of violations of 18 U.S.C. § 2252(a)(1) and (b)(1) (transportation of a visual depiction of a minor engaged in sexually explicit conduct); 18 U.S.C. § 2252(a)(2) and (b)(1) (receipt or distribution of a visual depiction of a minor engaged in sexually explicit conduct); 18 U.S.C. § 2252(a)(4)(B) and (b)(2) (possession of and access with intent to view a visual depiction of a minor engaged in sexually explicit conduct); 18 U.S.C. § 2252A(a)(1) and (b)(1) (transportation of child pornography); 18 U.S.C. § 2252A(a)(2)(A) and (b)(1) (receipt or distribution of child pornography); and 18 U.S.C. § 2252A(a)(5)(B) and (b)(2) (possession of and access with intent to view child pornography), are presently located at the SUBJECT PREMISES.

STATUTORY AUTHORITY

4. As noted above, this investigation concerns alleged violations of the following:

a. 18 U.S.C. § 2252(a)(1) and (b)(1) prohibit any person from knowingly transporting or shipping, or attempting or conspiring to transport or ship, any visual depiction using any means or facility of interstate or foreign commerce, or in or affecting interstate or foreign commerce, by any means, including by computer or mail, if the production of such visual depiction involved the use of a minor engaging in sexually explicit conduct and such visual depiction is of such conduct.

b. 18 U.S.C. § 2252(a)(2) and (b)(1) prohibit any person from knowingly receiving or distributing, or attempting or conspiring to receive or distribute, any visual depiction using any means or facility of interstate or foreign commerce, or that has been mailed or shipped or transported in or affecting interstate or foreign commerce, or which contains materials which have been mailed or so shipped or transported, by any means including by computer, or knowingly reproducing any visual depiction for distribution using any means or facility of interstate or foreign commerce, or in or affecting interstate or foreign commerce or through the mails, if the production of such visual depiction involved

the use of a minor engaging in sexually explicit conduct and such visual depiction is of such conduct.

c. 18 U.S.C. § 2252(a)(4)(B) and (b)(2) prohibit any person from knowingly possessing or accessing with the intent to view, or attempting or conspiring to possess or access with the intent to view, 1 or more books, magazines, periodicals, films, video tapes, or other matter which contain any visual depiction that has been mailed, or has been shipped or transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce, or which was produced using materials which have been mailed or so shipped or transported, by any means including by computer, if the production of such visual depiction involved the use of a minor engaging in sexually explicit conduct and such visual depiction is of such conduct.

d. 18 U.S.C. § 2252A(a)(1) and (b)(1) prohibit a person from knowingly mailing, or transporting or shipping using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce by any means, including by computer, any child pornography, as defined in 18 U.S.C. § 2256(8), or attempting or conspiring to do so.

e. Title 18, United States Code, Sections 2252A(a)(2)(A) and (b)(1) prohibit a person from knowingly receiving or distributing, or attempting or conspiring to receive or distribute, any child pornography or any material that

contains child pornography, as defined in 18 U.S.C. § 2256(8), that has been mailed, or using any means or facility of interstate or foreign commerce shipped or transported in or affecting interstate or foreign commerce by any means, including by computer.

f. 18 U.S.C. § 2252A(a)(5)(B) and (b)(2) prohibit a person from knowingly possessing or knowingly accessing with intent to view, or attempting or conspiring to do so, any material that contains an image of child pornography, as defined in 18 U.S.C. § 2256(8), that has been mailed, or shipped or transported using any means or facility of interstate or foreign commerce, or in or affecting interstate or foreign commerce, by any means, including by computer, or that was produced using materials that have been mailed or shipped or transported in or affecting interstate or foreign commerce by any means, including by computer.

BACKGROUND ON KIK AND KIK REPORTS

5. Kik Messenger (hereinafter "Kik") is a mobile application designed for chatting or messaging owned and operated by Kik Interactive, Inc. According to the publicly available document "Kik's Guide for Law Enforcement,"[1] to use this application, a user downloads the application to a mobile phone, computer, or other

[1] Available at: https://lawenforcement.kik.com/hc/en-us/categories/200320809-Guide-for-Law-Enforcement.

digital device via a service such as the iOS App Store, Google Play Store, Apple iTunes, or another similar provider. Once the application is downloaded and installed, the user is prompted to create an account and username. The user also creates a display name, which is a name that other users see when transmitting messages back and forth. Once the user has created an account, the user is able to locate other users via a search feature. While messaging, users can then send each other text messages, images, and videos.

6. According to "Kik's Guide for Law Enforcement," Kik users are also able to create chat groups with a limited number of individuals to communicate in a group setting and exchange text messages, images and videos. These groups are administered by the group creator who has the authority to remove and ban other users from the created group. Once the group is created, Kik users have the option of sharing a link to the group that includes all of their contacts or any other user. These groups are frequently created with a group name containing a hashtag (#) that is easily identifiable or searchable by keyword.

7. According to information provided to HSI by a Kik Law Enforcement Response Team Lead, Kik's Terms of Service prohibit Kik users from uploading, posting, sending, commenting on, or storing content that contains child pornography and/or child abuse images. The Terms of Service also provide that Kik may review, screen and delete user content at any time if Kik believes use of their services are in violation of the law. According to Kik, Kik has a strong business interest in enforcing their Terms of Service

and ensuring that their services are free of illegal content, and in particular, child sexual abuse material. Accordingly, Kik reports that it independently and voluntarily takes steps to monitor and safeguard their platform and that ridding Kik products and services of child abuse images are critically important to protecting their users, product, brand, and business interests.

8. At time of uploads in 2019, Kik was located in Ontario, Canada[2] and was governed by Canadian law. According to information contained in the "Kik Interactive, Inc. Child Sexual Abuse and Illegal Material Report and Glossary" (hereinafter Kik Glossary), which Kik provides when reporting information to law enforcement authorities, Kik is mandated to report to the Royal Canadian Mounted Police (RCMP) any images and/or videos that would constitute suspected child pornography under Canadian law which are discovered on the Kik platform. According to the Kik Glossary, Kik is typically alerted to suspected child pornography on Kik based on digital hash value matches to previously identified child pornography or through reports from other Kik users or third party moderators.

9. The RCMP has advised Homeland Security Investigations (HSI) agents that upon receiving a report from Kik related to suspected child pornography, the RCMP reviews the reported IP addresses of the Kik users contained in the Kik Reports to

[2] At the time of the report, Kik was a Canadian based company. Kik was bought by a US company in October 2019 and as of that date is subject to turning in all child exploitation leads to the National Center for Missing and Exploited Children (NCMEC)

determine their location. The RCMP then provides Kik Reports of Kik users in the United States to HSI in Ottawa, Canada, who in turn provides the Kik Reports to the HSI Cyber Crimes Center (C3) Child Exploitation Investigations Unit (CEIU) located in Fairfax, Virginia for analysis and dissemination.

BACKGROUND ON DISCORD AND DISCORD REPORTS

10. According to the National White Collar Crime Center (NW3C), Discord was launched in May 2015 by Hammer & Chisel as a free, proprietary Voice Over IP application, specifically marketed towards the "gaming" community. The service features a lightweight desktop application as well as a mobile app, and a user will typically use the same account across both platforms.

11. Discord provides free hosting for registered users to set up, configure, and customize their own communication servers, as well as voice calls and text chat rooms. Discord can be accessed via web browser at discord.gg or by installing an application for Windows, iOS, or Android device. New users register for the service with an email address, username, and password: after registering users have access to all of Discord's features.

12. Users of Discord choose an alphanumeric username, which is then combined with a pound symbol (#) as well as a string of four (4) or five (5) randomized numbers, producing a unique "tag". This tag cannot be changed. The tag is publicly

visible on an account's profile and can be used for a variety of networking purposes inside of Discord, such as a friend list, server whitelist[3], and blocking other users.

13. Discord users can link social media and entertainment service to their Discord account and can automatically integrate features of those applications into their Discord usage. All Discord profiles are public.

14. Discord protocol when dealing with child exploitation material is once Discord detects that child exploitation content is posted, the user is immediately removed from the Discord platform. A report is sent to the National Center for Missing and Exploited Children (NCMEC). Discord preserves the relevant data to the extent the law requires. Discord will not directly notify the user that the account has been removed and the user will not have access to their account. The Discord user will not be able to delete or alter the content of their account.

15. Discord stores identifying information (like the email address used to register an account and a history of IP addresses), and usage information (such as chat logs, login sessions, and device information). Discord also collects information from any third-party application linked to a user's profile, as well as advertising profiles on certain users.

[3] A whitelisted server is a **server that is only joinable by people that are put on a list**, named the whitelist. This means not just anyone can join and you have to apply to be put onto the list.

PROBABLE CAUSE

16. On or about December 2, 2019, HSI C3 sent HSI Bangor a Kik Report regarding the Kik account identified as "talkenhead77". I reviewed the Kik Report dated April 21, 2019 and learned that on April 21, 2019, "talkenhead77" used Kik to distribute one image of child pornography. The Kik Report contained information provided by the "talkenhead77" account user who provided the name associated with the account as "John John" and email address of "head66@yahoo.com". This email was not confirmed by Kik. The Kik Report showed the account was registered on February 2, 2019 and provided the registration client information as an iPhone.

17. I have learned that Kik was alerted to the child pornography through use of Microsoft's PhotoDNA technology. According to the Kik Glossary, Kik uses PhotoDNA to automatically scan user-uploaded files in order to flag images that may depict suspected child pornography and prevent such images from continuing to circulate through their application. When PhotoDNA detects a suspected child pornography file, it creates a Report and sends it to the Kik Law Enforcement team. According to information provided by a Kik Law Enforcement Response Team Lead, all suspected child pornography images and videos reported via a PhotoDNA Report, as well as any related user communications, are visually reviewed by a member of the Kik Law Enforcement Response team before a report is forwarded to law enforcement authorities. Kik trains employees comprising its Law Enforcement Response team on the legal

obligation to report apparent child pornography. The Team is trained on the Canadian statutory definition of child pornography and how to recognize it on Kik products and services. Kik voluntarily makes reports to law enforcement in accordance with that training. After Kik discovered the suspected child pornography, Kik removed the content from its communications system and closed the user's account.

18. Along with Kik's Report, Kik provided copies of the suspected child pornography image that they located to the RCMP. On December 2, 2019, I reviewed the very same image that Kik had provided with the Kik Report sent to the RCMP and forwarded to HSI. That image had previously been located, isolated, searched and viewed by Kik personnel before it was reported to the RCMP. I reviewed only the image that was previously located, isolated, searched and viewed by Kik personnel and observed that the image is child pornography as defined by Federal Law. Specifically, the image distributed by "talkenhead77" included the following:

a. **Image – uploaded by user: talkenhead77 from chat group http://profilepics.kik.com/0F3vNgqVhldDarN9dCRf13pH02o/orig.jpg:** This file is a color photograph of a prepubescent female, approximately eight (8) to nine (9) years of age, leaning against the wall on a bed completely nude, with a finger of one hand on her clitoris area and her other hand sticking one finger in her mouth. (attached under seal as Exhibit 1)

19. The information provided by Kik also included IP addresses associated with access to the "talkenhead77" account. Specifically, IP address 209.126.100.218 was used by "talkenhead77" on April 21, 2019 at 11:35:59 UTC, to distribute the child pornography image.

20. Kik also provided information stating that approximately one (1) hour after uploading the image of child pornography from IP address 209.126.100.218, Kik account "talkenhead77" was accessed from IP address 64.39.92.194. This was the last known IP address Kik user "talkenhead77" accessed.

21. A query of the American Registry for Internet Numbers (arin.net) online database revealed that IP address 64.39.92.194 was registered to BeeLine Cable and TV. On February 22, 2020, I issued an administrative summons to BeeLine Cable and TV, requesting subscriber information for IP address 64.39.92.194 for the date and time described above. A review of the results obtained from BeeLine stated that Lucas Vandine was the subscriber and the subscriber address as 52 Park Street, East Millinocket, Maine 04430, which is the address of the SUBJECT PREMISES. BeeLine also provided me with information stating that Vandine was the subscriber of that IP address since at least March 2019 until February 2020 when BeeLine sent their summons response.

22. A search of the Clear information database (a public records database that provides names, dates of births, addresses, telephone numbers, etc.) was conducted on

Vandine. These public records indicated Vandine has been associated with SUBJECT PREMISES since 2013 and as recently as May 2019.

23. I also conducted a check on Penobscot County deeds registration and learned that Lucas Vandine has a lien on the SUBJECT PREMISES and is the responsible party to pay property taxes in 2020.

24. A check with the State of Maine Division of Motor Vehicles revealed that Vandine lists his home address on his driver's license as the SUBJECT PREMISES.

25. On January 23, 2020, I received an investigative referral from the HSI C3, reporting a NCMEC [4] lead received from Discord regarding the user account identified as "bom#2499". I learned that "bom#2499" used Discord to distribute one image of child pornography on December 17, 2019. The NCMEC report contained data provided by the "bom#2499" account user who provided an email associated with the account as

[4] NCMEC is a nonprofit organization that provides services to families and professionals that relate to the abduction and sexual exploitation of children. NCMEC also operates the Cyber Tip line and the Child Victim Identification Programs to assist law enforcement officers and others in identifying and to rescuing victims of child exploitation and child pornography. As part of the NCMEC directives, the NCMEC works with electronic service providers (ESP) and electronic payment service providers to reduce the dissemination of child pornography images and or videos on the internet. When an ESP is made aware of suspected child pornography images and/or videos, the ESP representative may view the images and/or videos in question to determine if the images and or videos is child pornography and thus a violation of the ESP use agreement with the user(s). If the image and or video is deemed by the ESP representative to be child pornography, the ESP will file an electronic report with the NCMEC. The reporting ESP will provide in the NCMEC report samples of child pornography images and or videos, IP addresses captured at the date and time of the child pornography file being uploaded by the user, and any registration information (if available). NCMEC will then research more publicly available information based on the information provided to them by the ESP to determine, if possible, the identification and or geographic location of the user uploading the child pornography images and or videos.

bomsiuviet@gmail.com. NCMEC also provided the IP address from which the child pornography was distributed as 64.39.92.194.

26. I learned that once Discord detected the child pornography, Discord removed the user "bom#2499", preserved the data from the account and sent a report to NCMEC. NCMEC reviewed the report sent by Discord and determined the upload to be child pornography and forwarded the information to HSI C3.

27. On January 23, 2020, I reviewed the very same image that was provided by Discord to NCMEC and forwarded on to HSI. The image had previously been located, isolated, searched and viewed by Discord personnel before it was reported to NCMEC. I reviewed only the image that was previously located, isolated, searched and viewed by Discord personnel and observed one image to be child pornography as defined by Federal Law. Specifically, the image distributed by "bom#2499" included the following:

a. **Image – uploaded by user: bom#2499 filename: image0.jpg:**

This file is a color photograph of a male, approximately 10 to 12 years of age, laying on his stomach on a bed naked from the waist down. The male's scrotum is exposed, and he has what appears to be ejaculate covering his anus. (attached under seal as Exhibit 2)

28. On January 31, 2020, I issued an administrative summons to BeeLine Cable, requesting subscriber information for IP address 64.39.92.194 for the date and time it was used to upload the child pornography. A review of the results obtained

identified the subscriber as Lucas Vandine and the subscriber address as the SUBJECT PREMISES.

29. The information provided by Discord included the email address bomsiuviet@gmail.com. This email address was associated with another Discord account, talkinhed#8959, which led me to discover another referral from NCMEC regarding more child pornography uploads from the same IP address and email account associated with that Discord username.

30. On or about February 24, 2020, I learned that the Maine State Police Computer Crimes Unit (MSPCCU) had issued a subpoena to BeeLine Cable stemming from two (2) NCMEC reports sent to them on October 14, 2019. The NCMEC report identified IP address 64.39.92.194, with accompanying email address bomsiuviet@gmail.com, and username talkinhed#8959, as collectively uploading four (4) images of sexually explicit material of a minor with other Discord users on October 7 and October 27 of 2019.

31. On or about February 24, 2020, I reviewed the very same images that were provided by Discord to NCMEC and forwarded to HSI. Those images had previously been located, isolated, searched and viewed by Discord personnel before they were reported to NCMEC. I reviewed only the images that were previously located, isolated, searched and viewed by Discord personnel and observed one image to be child

pornography as defined by Federal Law. Specifically, the image distributed by identified Discord username talkinhed#8959, included the following:

a: **IMAGE – uploaded by user: talkinhed#8959: filename: image0.jpg**

This file is a color photograph of a six (6) to eight (8) year old prepubescent female with her torso, buttocks area, and legs nude sitting on all fours with only her back end exposed being penetrated by what appears to be an adult male penis. (attached under seal as exhibit 3)

32. On March 16, 2020, I conducted surveillance at the SUBJECT PREMISES and observed a red Ford Ranger pickup truck with a topper parked in the driveway bearing Maine license plate 166RZ. I ran the license plate through the Maine Division of Motor Vehicles and the vehicle came back to being registered to Lucas Vandine. While in the area of the SUBJECT PREMISES, I conducted a wireless survey and noted the only networks broadcasting were secure. On July 3, 2020, I again conducted surveillance of the SUBJECT PREMISES and saw the same red Ford Ranger pickup truck in the driveway.

33. Based on the above, I have probable cause to believe, and I do believe, that the SUBJECT PREMISES was used on two (2) separate occasions to upload and share child pornography via various social media platforms. The Kik account and the Discord accounts both come back to the same IP address 64.39.92.194, that has been assigned to the SUBJECT PREMISES since March of 2019 until February 2020 and more

specifically to Lucas Vandine. I also have probable cause to believe that based on the fact that both Kik and Discord are applications that are primarily run on mobile devices such as cell phones, any persons residing at the SUBJECT PREMISES, mainly, Lucas Vandine, be subject to search at the SUBJECT PREMISES and/or within the District of Maine at the time of the execution of the search warrant.

SPECIFICS OF SEARCH AND SEIZURE OF COMPUTER SYSTEMS

34. Based upon my training and experience and information relayed to me by agents and others involved in the forensic examination of computers and mobile devices, I know that data can be stored on a variety of systems and storage devices, including external and internal hard drives, flash drives, thumb drives, micro SD cards, macro SD cards, DVDs, gaming systems, SIM cards, cellular phones capable of storage, floppy disks, compact disks, magnetic tapes, memory cards, memory chips, and online or offsite storage servers maintained by corporations, including but not limited to "cloud" storage. I also know that during the search of the premises it is not always possible to search computer equipment and storage devices for data for a number of reasons, including the following:

a. Searching computer systems is a highly technical process which requires specific expertise and specialized equipment. There are so many types of computer hardware and software in use today that it is impossible to bring to the search site all of the technical manuals and specialized equipment necessary to

conduct a thorough search. In addition, it may also be necessary to consult with computer personnel who have specific expertise in the type of computer, software application, or operating system that is being searched;

b. Searching computer systems requires the use of precise, scientific procedures which are designed to maintain the integrity of the evidence and to recover "hidden," erased, compressed, encrypted, or password-protected data. Computer hardware and storage devices may contain "booby traps" that destroy or alter data if certain procedures are not scrupulously followed. Since computer data is particularly vulnerable to inadvertent or intentional modification or destruction, a controlled environment, such as a law enforcement laboratory, is essential to conducting a complete and accurate analysis of the equipment and storage devices from which the data will be extracted;

c. The volume of data stored on many computer systems and storage devices will typically be so large that it will be highly impractical to search for data during the execution of the physical search of the premises; and

d. Computer users can attempt to conceal data within computer equipment and storage devices through a number of methods, including the use of innocuous or misleading filenames and extensions. For example, files with the extension ".jpg" often are image files; however, a user can easily change the extension to ".txt" to conceal the image and make it appear that the file contains

text. Computer users can also attempt to conceal data by using encryption, which means that a password or device, such as a "dongle" or "keycard," is necessary to decrypt the data into readable form. In addition, computer users can conceal data within another seemingly unrelated and innocuous file in a process called "steganography." For example, by using steganography a computer user can conceal text in an image file which cannot be viewed when the image file is opened. Therefore, a substantial amount of time is necessary to extract and sort through data that is concealed or encrypted to determine whether it is contraband, evidence, fruits, or instrumentalities of a crime.

35. Based on my own experience and my consultation with other agents who have been involved in computer searches, searching computerized information for contraband, evidence, fruits, or instrumentalities of a crime often requires the seizure of all of a computer system's input and output peripheral devices, related software, documentation, and data security devices (including passwords), so that a qualified computer expert can accurately retrieve the system's data in a laboratory or other controlled environment. There are several reasons that compel this conclusion:

a. The peripheral devices that allow users to enter or retrieve data from the storage devices vary widely in their compatibility with other hardware and software. Many system storage devices require particular input/output devices in order to read the data on the system. It is important that the analyst be able to

properly re-configure the system as it now operates in order to accurately retrieve the evidence listed above. In addition, the analyst needs the relevant system software (operating systems, interfaces, and hardware drivers) and any applications software which may have been used to create the data (whether stored on hard drives or on external media), as well as all related instruction manuals or other documentation and data security devices; and

b. In order to fully retrieve data from a computer system, the analyst also needs all magnetic storage devices, as well as the central processing unit (CPU).

36. Additionally, based upon my training and experience and information related to me by agents and others involved in the forensic examination of computers, I know that routers, modems, and network equipment used to connect computers to the Internet often provide valuable evidence of, and are instrumentalities of, a crime. This is equally true of so-called "wireless routers," which create localized networks that allow individuals to connect to the Internet wirelessly. Though wireless networks may be "secured" (in that they require an individual to enter an alphanumeric key or password before gaining access to the network) or "unsecured" (in that an individual may access the wireless network without a key or password), wireless routers for both secured and unsecured wireless networks may yield significant evidence of, or serve as instrumentalities of, a crime—including, for example, serving as the instrument through

which the perpetrator of the Internet-based crime connected to the Internet and, potentially, containing logging information regarding the time and date of a perpetrator's network activity as well as identifying information for the specific device(s) the perpetrator used to access the network. Moreover, I know that individuals who have set up either a secured or unsecured wireless network in their residence are often among the primary users of that wireless network.

ELECTRONIC DEVICES, ELECTRONIC STORAGE, AND FORENSIC ANALYSIS

37. As described above and in Attachment A, this application seeks permission to search for DEVICES and seize data and images that the DEVICES might contain, which pertain to violations of 18 U.S.C. §§ 2252 and 2252A. Some electronic data on the DEVICES may take the form of files, photographs, documents, and other data that is user-generated. Other data might become meaningful only upon forensic analysis. There is probable cause to believe that this forensic electronic evidence might be on the DEVICES because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file).

b. A person with appropriate familiarity with how an electronic device

works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.

c. The process of identifying the exact electronically stored information on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer or cell phone is evidence may depend on other information stored on the computer or cell phone and the application of knowledge about how the device behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

d. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

38. Based on my knowledge, training, and experience, I know that:

a. Files or remnants of files can be recovered months or even years after they have been downloaded onto an electronic device, deleted, or viewed via the Internet. Electronic files downloaded to an electronic device can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is because when a person "deletes"

a file from an electronic device, the data contained in the file does not necessarily disappear; rather, that data is no longer indexed but remains on the storage medium until it is overwritten by new data.

b. Wholly apart from user-generated files, electronic devices often contain electronic evidence of how the device has been used, what it has been used for, and who has used it. This evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and other files.

c. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache." These files are only overwritten as they are replaced with more recently viewed Internet pages or if a user takes steps to delete them.

d. As further described in Attachment B, this application seeks permission to locate not only data that might serve as direct evidence of the crimes described on the warrant, but also for evidence that establishes how the DEVICES were used, the purpose of its use, who used it, where it was used, and when. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence.

e. Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the DEVICES

consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrant.

f. The government intends to make and retain a full image copy of the seized media, so that a copy of the evidence, rather than the original evidence, can be examined. The government will seize and retain both the original evidence and any copies of this evidence. This procedure will ensure that the original evidence remains intact.

REQUEST FOR SEALING OF APPLICATION/AFFIDAVIT

39. It is respectfully requested that this Court issue an order sealing, until further order of this Court, all papers submitted in support of this Application, including the Application, Affidavit, and Search Warrant, and the requisite inventory notice (with the exception of one copy of the warrant and the inventory notice that will be left at the SUBJECT PREMISES). Sealing is necessary because the items and information to be seized are relevant to an ongoing investigation and not all of the targets of this investigation will be searched at this time. Based upon my training and experience, I have learned that online criminals actively search for criminal affidavits and search warrants via the Internet and disseminate them to other online criminals as they deem appropriate, *i.e.*, post them publicly online through forums. Premature disclosure of the

contents of this Affidavit and related documents may have a significant and negative impact on this continuing investigation and may jeopardize its effectiveness by alerting potential targets to the existence and nature of the investigation, thereby giving them an opportunity to flee, or to destroy or tamper with evidence.

CONCLUSION

40. Based on the foregoing, there is probable cause to believe that the federal criminal statutes cited herein have been violated, and that the contraband, property, evidence, fruits and instrumentalities of these offenses, more fully described in Attachment B, are located at the locations described in Attachment A. I respectfully request that this Court issue a search warrant for the locations described in Attachment A, authorizing the seizure and search of the items described in Attachment B.

41. I am aware that the recovery of data by a computer forensic analyst takes significant time. For this reason, the "return" inventory will contain a list of only the tangible items recovered from the premises. Unless otherwise ordered by the Court, the return will not include evidence later examined by a forensic analyst.

Daniel E. Zaehringer
Special Agent
Homeland Security Investigations

Sworn to telephonically and signed electronically in accordance with the requirements of Rule 4.1 of the Federal Rules of Criminal Procedure

Date: Jul 16, 2020,

City and state: Bangor, Maine

Judge's signature

John C Nivson U.S. Magistrate Judge

Printed name and title